PATENT COOPERATION TREATY

WO 2005/029223
PCT/US2004/029470

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
TRANSMITTAL OF COPY OF INTERNATIONAL
APPLICATION AS PUBLISHED OR REPUBLISHED

To:

ADELI, Mani
Stattler Johansen & Adeli
P.O. Box 51860
Palo Alto, CA 94303-0728
ETATS-UNIS D'AMERIQUE

Date of mailing *(day/month/year)* 23 February 2006 (23.02.2006)	
Applicant's or agent's file reference APLE.P0011PCT	**IMPORTANT NOTICE**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2004/029470	10 September 2004 (10.09.2004)	18 September 2003 (18.09.2003)

Applicant
APPLE COMPUTER, INC. et al

The International Bureau transmits herewith the following documents:

☐ copy of the international application as published by the International Bureau on under No. WO

☑ copy of international application as republished by the International Bureau on 23 February 2006 (23.02.2006) under No. WO 2005/029223
For an explanation as to the reason for this republication of the international application, reference is made to INID codes (15), (48) or (88) (*as the case may be*) on the front page of the attached document.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Ellen Moyse
Facsimile No.+41 22 740 14 35	Facsimile No.+41 22 338 89 75

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 March 2005 (31.03.2005)

PCT

(10) International Publication Number
WO 2005/029223 A3

(51) International Patent Classification:
H04L 9/36 (2006.01) *G06F 11/30* (2006.01)
G06F 11/22 (2006.01)

(21) International Application Number:
PCT/US2004/029470

(22) International Filing Date:
10 September 2004 (10.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/666,847 18 September 2003 (18.09.2003) US

(71) Applicant (*for all designated States except US*): **APPLE COMPUTER, INC.** [US/US]; One Infinite Loop, Mail Stop: 38-PAT, Cupertino, CA 95014 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **KIEHTREIBER, Perry** [AT/US]; 1509 Walnut Drive, Campbell, CA 95008 (US). **BROUWER, Michael** [NL/US]; 141 Red River Way, San Jose, CA 95136 (US).

(74) Agent: **ADELI, Mani**; Stattler Johansen & Adeli, P.O. Box 51860, Palo Alto, CA 94303-0728 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

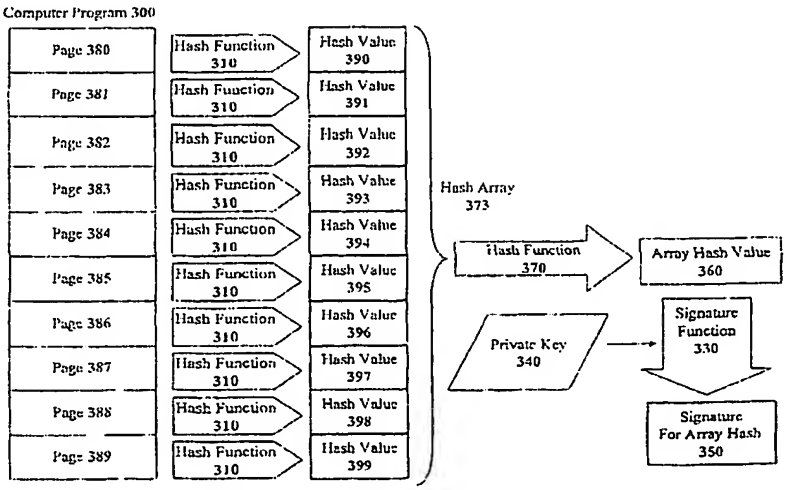
(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
23 February 2006

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR INCREMENTAL CODE SIGNING



(57) Abstract: The present invention discloses a method for quickly and easily authenticating large computer program (300). The system operates by first sealing the computer program with digital signature (350) in an incremental manner. Specifically, the computer program is divided into a set of pages (380) and a hash value (310) is calculated for each page (390). The set of hash values (390) is formed into a hash value array (373) and then the hash value array is then sealed with a digital signature (350). The computer program (300) is then distributed along with the hash value array (373) and the digital signature (350). To authenticate the computer program (300), a recipient first verifies the authenticity of the hash value array (373) with the digital signature (350) and a public key. Once the hash value array (373) has been authenticated, the recipient can then verify the authenticity of each page (380) of the computer program (300) by calculating a hash of a page (380) to be loaded and then comparing with an associated hash value (390) in the authenticated hash value array (373). If the hash values do not match, then execution may be halted.

WO 2005/029223 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/29470

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) : H04L 9/36; G06F 11/22, 11/30
US Cl. : 713/187, 190; 726/22
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/160, 161, 176, 181; 726/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	EP 0752786 A1 THOMSON CONSUMER ELECTRONICS, INC.) 08 January 1997 (08.01.97), page 7, lines 20-21, 32-33; page 8, lines 2 and 5-14; page 11, lines 31-39 and 53-59; figure 1, item 11; figure 7, steps 41, 46, 51, and 53; figure 10, steps 124, 126, 136, 138, 140, 148, 150, and 152; figure 11, step 1244.	1, 3, 6, 8-11, 13-15, 17-20 --- 2, 4, 5, 7, 12, 16
Y	SCHNEIER, B.Applied Cryptography, Second Edition: Protocols, Algorigthms, and Source Code in C. 1996, section 18.7, pages 442-445.	2, 4, 5, 12
Y	US 2002/0194484 A1 (BOLOSKY et al) 19 December 2002 (19.12.2002), paragraphs [0005], [0061], and [0070]; figure 3, item 358; figure 4, item 402.	7, 16
A	WO 01/63385 A1 (NCIPHER CORP. LTD.) 30 August 2001 (30.08.01), page 7, lines 5-12; figure 5, items 22, 24, 302, and 306.	1-20
A	WO 02/41147 A1 (DIGITAL TRANSIT) 23 May 2002 (23.05.02), page 58, lines 925; figure 12, items 1408, 1410, 1412, and 1414.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 December 2005 (09.12.2005)	27 DEC 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Justin T. Darrow Telephone No. 571-272-3801

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/29470

Continuation of B. FIELDS SEARCHED Item 3:
EAST(US-PGPUB; USPAT); EAST(EPO; JPO; DERWENT)
search terms: divide, split, separate, part, segment, partition, block, subblock, program, software, instructions, executable, operating system, hash, array, vector, matrix, set, sign, signature, SHA, distribute, transmit, send, transfer, forward, communication, receive, download, uplink, upload, public key, asymmetric key, verify, authenticate, confirm, validate, error, alert, fault